

Top Ten Security Issues Voice over IP (VoIP)

Top Ten Security Issues with Voice over IP (VoIP)

Voice over IP (VoIP), the use of the packet switched internet for telephony, has grown substantially in the past ten years. Securing VoIP has many challenges that do not exist in the public switched telephone network (PSTN), a circuit switched system. VoIP is an application running on the internet, and therefore inherits the internet's security issues. It is important to realize that VoIP is a relatively young technology, and with any new technology, security typically improves with maturation. This paper identifies the top ten security issues commonly found in a corporate VoIP implementation, the methods to combat them, and security issues not fully addressed by the industry.

History of telephone hacking

The telephone network has historically been a target of hackers. The term "phreaking", the act of telephone hacking, became prevalent in the 1970's and 80's. A subculture of telephony hackers developed methods to illegally control telephone networks. The intent of these intrusions varied substantially. Some simply viewed phreaking as a hobby, with no real intent to do damage. Others gained illegal access to bypass toll charges and obtain free long distance service. Last, the aim of certain individuals is more devious in nature. Activities such as call diverting, rerouting, and eavesdropping are all security issues of the PSTN network. Unfortunately, these same issues exist within VoIP telephony.

An introduction to VoIP

VoIP leverages the internet as an infrastructure for voice communications. Data packets carry voice in the same manner as general internet traffic. This configuration is more efficient than the PSTN network. VoIP can use one shared broadband circuit for many packet switched services; data, voice, and even video teleconferencing. Within an office environment, VoIP implementations often converge with the existing data network. While this consolidation reduces costs, it also places greater performance and security demands on the network switches. One cabling infrastructure, and one set of switches, manages network connectivity for both voice and data services. Some networks further collapse services such as wireless and video teleconferencing into the switch stack. Sophisticated layer three switches identify devices either as phones, computers, or wireless access points, and then assign these devices to the appropriate virtual local area network. Once on the correct virtual LAN, they obtain an IP assignment to the correct network. This device categorization is important for a number of reasons. Assigning devices to virtual networks applies security parameters distinctly based on network type, a good security practice. Additionally, categorizing devices allows the switch to prioritize one group's traffic over another, a process called quality of service (QoS), which is very important in protecting call quality in a converged system (Stredicke, 2007).

VoIP phone systems look and feel just like network servers. In fact, many of these systems run Microsoft Windows 2003 / 2008 Server, or perhaps a version of Linux. VoIP offers integration between the computer and phone, an application called unified communications (UC). UC integrates voicemail into email, provides intelligent call forwarding services, simplifies conference calling, and may offer a computer “dashboard” application into the phone system. All of these technological improvements open the telephony system to new kinds of vulnerabilities that simply don’t exist in traditional telephony. Solid security is not optional; it is a prerequisite to VoIP.

Top Ten Security Issues

Now that we have background information on VoIP, and how convergence creates both opportunities and problems, let us analyze the top ten security issues commonly found with a corporate VoIP implementation.

Problem # 1: VoIP traffic might be internet bound.

Routing traffic over the internet is inherently less secure than placing a call over traditional circuit switched networks. The internet is a dangerous place, and packet sniffers can grab unencrypted traffic. Some solutions utilize virtual private network (VPN) tunnels to connect a remote phone to the corporate office phone system. With two limitations, this solution works well. VPN’s can take some time to setup, so prior to placing or receiving phone calls, the VPN connection would need to be up and running. This process can take as much as thirty seconds with client initiated VPN. Second, VPN is a hardware intensive service. If the strain of encrypting and decrypting traffic on the VPN appliance becomes burdensome, the result may be delayed VoIP packets. This will cause delay and jitter on the VoIP phone. In short, intra-office communications aside, voice traffic running over the internet is best protected via encryption, and the speed of the VPN process requires special attention when handling VoIP traffic.

Problem # 2: Gateway security options for VoIP are limited.

Securing VoIP traffic at the firewall level presents certain challenges. First, not all firewalls are VoIP aware. An older firewall may not recognize VoIP protocols such as SIP, MGCP or Cisco’s SCCP protocol, and incorrectly block this traffic. Second, many firewalls actively scan traffic packets as an intrusion detection / prevention system. Typically, this sort of scanning is not recommended because of the time-critical nature of VoIP traffic. Experts set a threshold of 300 milliseconds to setup a call, and 100 milliseconds end-to-end packet delivery. “Given these performance constraints, many security measures implemented in traditional data networks are simply not applicable to VoIP” (Epps, 2006). The industry does not have a good answer to active packet scanning on VoIP implementations at this time. The best advice is to attempt full

traffic scanning, measure the results, and determine if your IDS/IPS system is able to scan without performance issues.

Problem # 3: Patching problems.

Updating VoIP endpoints presents a number of challenges. First, many technology administrators might forgo patching phones as unnecessary. Legacy phone handsets did not require software updates, and many incorrectly assume security patches do not exist for phones. Second, many organizations do not have downtime windows set up for telephony. Administrators find that they do not have the same access to maintenance downtime with telephony as they do with data services. Finally, the patching system for many VoIP endpoints is far too simple, unsecure, and, in certain cases, dangerous. Many VoIP phones use the trivial file transfer protocol (TFTP) to update software or firmware. In many cases this is set up to occur without authentication. Additionally, the criterion to install the update often only requires the presence of a different file. In other words, if the file differs from what is currently running on the phone, it will install. A compromised TFTP server would allow a hacker to place any file in the upload directory, and it would be loaded onto the handset (Thermos, 2007). This could cause a complete system outage. The moral to the patching story is straightforward. VoIP phone systems require diligent patching of the core call management system, voicemail system, infrastructure components, and endpoints, to maintain a high level of security.

Problem # 4: VoIP security is only as reliable as the underlying network security.

One simple cause of security issues with a VoIP implementation has little to do with the telephony system. If an existing network has security vulnerabilities, these can be exploited once VoIP is implemented.

Many experts recommend an independent security assessment in advance of a VoIP deployment. Areas of concern include gateway security, firewall configuration, patching procedures, periodic syslog review, and wireless security. It is far more difficult to remediate security issues after an installation, so be sure your security house is in order prior to implementation.

Problem # 5: Many call processing systems run on common operating systems, and they have their own security issues to worry about.

In the same light as problem number four on our list, phone system vendors who leverage industry recognized operating systems inherit the operating systems' vulnerabilities. A phone system running on Microsoft's Windows 2008 server requires regular updates to resolve newly discovered critical issues (Lacy, 2006). In many cases this will require a reboot and phone

system downtime. Some vendors now realize that the ease of using a market leading operating system is not worth the security trade-off.

For example, leading VoIP telephony vendor Cisco Systems is moving its Call Manager product from Windows Server products to Linux. Many in the industry believe that this move will address many security and patching issues for Cisco. Additionally, versions of *nix operating environments make it easier to turn off unwanted services. These “locked down” versions of the operating system offer certain safeguards over the fully functional off-the-shelf equivalents. Remember, all parts of the phone system require maintenance and attention. Simply updating the phone system software is not enough. Patch the underlying environment with manufacturer supplied updates.

Problem # 6: Denial of Service (DoS) takes down telephony.

Out of the box VoIP implementations may leave TCP/UDP ports unnecessarily open and without sufficient monitoring. These, along with other default services, could create a habitat suitable for a DoS or distributed DoS attack. A distributed DoS attack is a concerted, coordinated effort to flood a network with requests. Though the attacked network may not be penetrated, these attacks can “busy” a system, rendering it unusable. To combat these attacks, security experts must ensure that unnecessary ports and services are shut down, and that the network is properly patched for newly discovered vulnerabilities.

Problem # 7: Eavesdropping on calls using VOMIT or SipTap.

Voice over Misconfigured Internet Telephones (VOMIT) is a software tool that siphons voice TCP/IP packets running on Cisco’s phone system, and its proprietary protocol known as skinny (SCCP). It operates on the network by grabbing packets, which can convert to a wave voice file for listening (Persky, 2007).

More recently, a product called SipTap has demonstrated the capacity to intercept unencrypted SIP based VoIP traffic. SipTap has grabbed the attention of the VoIP community. SipTap siphons not only voice calls, but also caller ID style information, labeling the call originator, recipient, duration, and time. Corporate espionage via a product like SipTap is a dangerous proposition (Cox, 2009).

The only existing method to prevent this sort of eavesdropping is to properly secure access to the call management system, and to encrypt voice data. Even if a network were self-contained and secure, an internal threat, such as a disgruntled employee, could use an application like SipTap to snoop on internal conversations. Again, the method to combat this is encryption if the network can support this from a performance viewpoint.

Last, the industry has general unresolved issues with SIP. SIP is popular because it is open and integrates easily. As VoIP and SIP grow, it is likely that SIP vulnerabilities and exploits will continue to rise. Future versions of SIP will likely address security issues.

Problem # 8: Spam over IP telephony (SPIT).

Spam over IP telephony (SPIT), involves prerecorded, unsolicited messages sent to your VoIP handset. SPIT owes its existence to the standard communications protocol called Session Initiated Protocol (SIP). SIP acknowledges the presence of a VoIP handset. Dialer programs can deliver an unsolicited programmed message, and have a better chance of a recipient picking up the call (Phithakkitnukoon, 2008). SPIT carries with it other risks, such as DoS attacks, and the unauthorized use of resources (bandwidth), making SPIT much more than a nuisance. SPIT's effects are lessened by a solid patch management solution, VoIP enabled firewalls are likely capable of identifying SPIT, and create an authentication mechanism to identify true authorized callers. In short, the philosophy of combating SPIT is very similar to current day methods used to combat SPAM; it is impossible to stop it, you can only hope to control it.

Problem # 9: More ports open = more ports to secure.

While the infrastructure equipment may remain unchanged, VoIP complicates network traffic flow with many new ports, rules, and virtual networks. A communications expert must carefully map out TCP and UDP traffic rules, the method by which this traffic traverses the internal network, as well as the resulting implications to the corporate wide area network and remote access policies.

The best advice is to carefully plan an implementation ahead of the installation. The existing firewall configuration rule set should be available, and a certified network communications engineer should document proposed changes to the configuration to support the VoIP implementation. As with any major infrastructure change, only a minimum number of ports should be opened on the firewall to facilitate services.

Problem # 10: Wireless phones require advanced wireless security.

Many VoIP phone systems offer wireless handsets for mobility. These implementations often make use of existing 802.11x wireless solutions. Weak wireless security exposes VoIP vulnerabilities.

Do not give hackers the opportunity to wirelessly access your network. The best wireless solutions require centralized network authentication, in addition to wireless encryption. If your wireless supports authentication by radius, or direct integration with directory services such as Microsoft Active Directory, implement this wireless security ahead of a VoIP deployment. If

you are using lower end wireless access points, you should at the very least use WPA (a form of encryption) over WEP encryption, although a novice hacker can easily defeat WEP.

Concluding Remarks and Tips to Secure VoIP

VoIP is now prevalent in corporate America. All too often, products release to market without well thought out security. Unfortunately, this has largely proven true with VoIP. While you should not fear a VoIP implementation, make sure your security house is in order prior to folding voice services into your data network. I leave you with the following tips summarizing the recommendations supplied in this paper.

Tip # 1 – Perform a security audit ahead of the implementation. Remediate vulnerabilities prior to your VoIP implementation.

Tip # 2 – If you cannot afford a security audit, have your firewall administrator review the existing configuration, propose necessary changes for VoIP, and have the telephony vendor review for accuracy. Further, use this as an opportunity to shut down unneeded ports on your firewall.

Tip # 3 – Make sure your firewall is VoIP aware. If not, you should upgrade it ahead of time.

Tip # 4 - Plan on establishing VPN tunnels for any endpoint connectivity outside of the corporate office.

Tip # 5 – If you use an IDS/IPS, you can try to run VoIP behind it, but should have a backup plan if the results are not acceptable. This plan would include steps to move the phone system to a different un-scanned subnet. Remember, active packet scanning can cause jitter and delay on your VoIP phone.

Tip # 6 – Have your telephony vendor write up a recommended patching methodology and training program for IT staff. Make sure that handsets are included in the program.

Tip # 7 – If a general patching program does not exist, have your IT director write up a patching policy for all other aspects of the network.

Tip # 8 – Include your VoIP servers in the tape backup schedule. Without a backup, you would not be able to restore telephony in the event of a disaster.

Tip # 9 – SIP may be popular, but it may not be worth the risk. If you have a choice, it may be worth using a proprietary protocol, such as Cisco's SCCP.

Hopefully this paper provides a solid foundation for a secure VoIP implementation. If you have any questions, the author's email address is mruck@designdata.com.

Works Cited

Cox, P. (2009) SIPTap a SIP Call Monitoring Demonstrator. Voipcode.org website.

Epps, D., Tanner, S., & Silva, C. (2006, May). Can VoIP Secure Itself for the Next Technology Wave?. *Information Systems Security*, 15(2), 9-15.

Phithakkitnukoon, S., Dantu, R., & Baatarjav, E. (2008, May). VoIP Security — Attacks and Solutions. *Information Security Journal: A Global Perspective*, 17(3), 114-123.

Lacy, S. (2006, June 13). Is Your VoIP Phone Vulnerable?. *Business Week Online*,

Persky, D. (2007). VoIP Security Vulnerabilities. *Sans Institute 2007*. Retrieved July 13, 2009

Stredicke, C. (2007, August). Why VoIP security matters. *Communications News*, 44(8), 30-32.

Thermos, P. (2009, May). Evaluating the Security of Enterprise VoIP Networks. *Computer.org*.